Billing Code: 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Multistakeholder Process on Promoting Software Component Transparency

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of Open Meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene meetings of a multistakeholder process on promoting software component transparency. This Notice announces the first meeting, which is scheduled for July 19, 2018.

DATES: The meeting will be held on July 19, 2018, from 10:00 a.m. to 4:00 p.m., Eastern Daylight Time.

ADDRESSES: The meeting will be held at the American Institute of Architects, 1735 New York Ave., N.W., Washington, DC 20006.

FOR FURTHER INFORMATION CONTACT: Allan Friedman, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230; telephone: (202) 482-4281; email: afriedman@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs: (202) 482-7002; email: press@ntia.doc.gov.

SUPPLEMENTARY INFORMATION:

Background: Since 2015, the National Telecommunications and Information Administration has sought public comment on several matters around information and cyber policy and security, the Internet of Things (IoT), and the health of the digital ecosystem. In

2015, NTIA issued a Request for Comment to "identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers."[1] In a separate but related matter in April 2016, NTIA, along with the Department's Internet Policy Task Force, sought comments on the "benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things."[2] Lastly, as part of Executive Order 13800, NTIA requested comments on "Promoting Stakeholder Action Against Botnets and Other Automated Threats."[3]

Several themes emerged from these three public consultations. Many stakeholders emphasized the importance of community-led, consensus-driven, and risk-based solutions to address information security challenges, highlighting the role NTIA should play in convening multistakeholder processes. In the digital ecosystem, particular challenges were identified: understanding and handling vulnerability information, addressing the insecurities in the growing IoT marketplace, and fostering a secure development lifecycle. NTIA has convened two multistakeholder processes to address these policy and market challenges. The first focused on how to promote collaboration around communicating vulnerability information, and the second

[1] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360, Docket No. 150312253-5253-01 (Mar. 19, 2015), *available at*: https://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.

[2] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956, Docket No 160331306-6306-01 (Apr. 5, 2016), *available at*: https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.

[3] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Promoting Stakeholder Action Against Botnets and Other Automated Threats, 82 Fed. Reg. 27042, Docket No. 170602536-7536-01 (Mar. 19, 2015), *available at*: https://www.ntia.doc.gov/files/ntia/publications/fr-ntia-cyber-eo-rfc-06132017.pdf.

helped vendors and consumers understand policy and market concerns related to patching vulnerabilities.

The next initiative will focus on promoting software component transparency. Stakeholders will engage in an open and transparent process to explore the benefits and any potential risks of greater transparency. They may focus on incentives and barriers to adoption of transparency practices. The scope could include policy and international components. Transparency-driven solutions need not be prescriptive or regulatory, and can accommodate an ecosystem without a one-size-fits-all approach. The goal of this initiative is to foster a market that offers greater transparency on software components.

Most modern software is not written completely from scratch, but includes existing components, modules, and libraries from the open source and commercial software world. Modern development practices such as code reuse, and a dynamic IT marketplace with acquisitions and mergers, make it challenging to track the use of software components. The Internet of Things compounds this phenomenon, as new organizations, enterprises and innovators take on the role of software developer to add "smart" features or connectivity to their products. While the majority of libraries and components do not have known vulnerabilities, many do, and the sheer quantity of software means that some software products ship with vulnerable or out-of-date components. Many technical solutions to aid in this have already been developed by industry and the standards community.

Vendors and developers also would find software component data useful. Cataloging the inputs to a software product is recognized as an important part of a secure development life

cycle.[4] Indeed, many organizations have developed internal processes to capture and manage this data for security purposes. Many others do so to manage licensing issues around third-party software components and intellectual property rights. Communicating information about the underlying components can be a strong security signifier, while still protecting the valuable intellectual property and source code in software and devices.

The importance of transparency in information security is widely recognized, and the notion of transparency around components of software and connected devices is not new. Academics identified the potential value of a "software bill of materials" as far back as 1995,[5] and there are a growing number of commercial solutions for security, licensing, and asset management. The International Standards Organization (ISO) first standardized software identification (SWID) tags in 2009.[6] In 2015, NIST published Guidelines for the Creation of Interoperable Software Identification (SWID) Tags,[7] and their use has been slowly increasing.

[4] The Software Assurance Forum for Excellence in Code (SAFECode), an industry consortium, has released a report on third party components that cites a range of standards. *Managing Security Risks Inherent in the Use of Third-party Components*, SAFECode (May 2017), *available at* https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf.

[5] Leblang D.B., Levine P.H., Software configuration management: Why is it needed and what should it do? In: Estublier J. (eds) Software Configuration Management Lecture Notes in Computer Science, vol. 1005, Springer, Berlin, Heidelberg (1995).

[6] ISO/IEC 19770 "Software Identification Tag," originally published in 2009, updated in 2015, https://www.iso.org/standard/65666.html.

[7] U.S. Department of Commerce, Guidelines for the Creation of Interoperable Software Identification (SWID) Tags, National Institute of Standards and Technology Internal Report 8060 (Dec. 2015), a*vailable at:* https://csrc.nist.gov/csrc/media/publications/nistir/8060/final/documents/nistir_8060_draft_fourth.pdf.

The open source community has also developed the Software Package Data Exchange.[8] This process will explore successful examples of use, and market barriers to increased adoption. From the perspective of the enterprise customer, it is hard to defend what one does not know. Transparency itself is not sufficient; the data must be useful and actionable. Understanding what is on an enterprise network is a key part of a security program. Having data about software components allows the enterprise customer to better understand the risks of potentially vulnerable software and devices.

Any conversation around transparency must include a discussion of the needs of the diverse set of enterprise software users. Data about the underlying code can help both the customer and the vendor. It should be incorporated into a security-mature organization's existing vulnerability management solutions, and can help foster further innovation. Having access to this data can help organizations mitigate concerns around orphaned devices and products, and lower the risks of investing in new products by increasing capabilities to deal with future security issues.

NTIA will act as the convener, but stakeholders will drive the outcomes. Stakeholders will determine how to scope and organize the work through subgroups or other means. Success of the process will be evaluated by the extent to which broader findings on software component transparency are implemented across the ecosystem.

This multistakeholder process is not a standards development process and will not supplant ongoing standards efforts or discussions. NTIA will frame the initial conversation around the policy and market considerations for greater software component transparency. NTIA encourages cross-sector participation as this will help to prevent sector-specific solutions

[8] More information on the Software Package Data Exchange project is available at https://spdx.org.

that could fragment the marketplace. NTIA encourages discussion of approaches and considerations from diverse sectors such as the medical device community, where the applicability of a "bill of materials" has garnered increased discussion and interest.[9] This approach can promote a more efficient and adaptive marketplace for new products.

Matters to Be Considered: The July 19, 2018, meeting will be the first in a series of NTIA-convened multistakeholder discussions on promoting software component transparency. Subsequent meetings will follow on a schedule determined by those participating in the first meeting. Stakeholders will engage in an open, transparent, and consensus-driven process to understand the range of issues involved. The multistakeholder process will involve hearing and understanding the perspectives of diverse stakeholders, explicitly sharing the perspectives of a range of software and IoT vendors and enterprise customers from across the digital economy.

The July 19, 2018, meeting is intended to bring stakeholders together to share the range of views on software component transparency, and to establish more concrete goals and structure of the process. The objectives of this first meeting are to: 1) share the perspectives and concerns of both the vendor and enterprise customer communities; 2) discuss and acknowledge what is already working; 3) explore obstacles and challenges for greater transparency and better risk decisions; 4) identify promising areas of potential collaboration; 5) engage stakeholders in a discussion of logistical issues, including internal structures such as a small drafting committee or various working groups, and the location and frequency of future meetings; and 6) identify concrete goals and stakeholder work following the first meeting. These topics could include, but are in no way limited to, an inventory of existing statutory, policy, regulatory, and market efforts to increase software component transparency; identification of incentives and disincentives for

market adoption of approaches for software component transparency; exploration of statutory, policy, and regulatory activities that may inhibit adoption; accessible high-level guidance for strategic decision-makers; and review of international approaches to understand statutory, policy, and regulatory environments to understand effects on market adoption.

The main objective of further meetings will be to encourage and facilitate continued discussion among stakeholders to map the range of issues, and develop a consensus view for some determined aspects of transparency. This discussion may include the appropriate scope of the initiative and circulation of stakeholder-developed drafts. Stakeholders may also agree on procedural work plans for the group, including additional meetings or modified logistics for future meetings. NTIA suggests that stakeholders consider setting clear deadlines for working drafts and a phase for external review of such drafts, before reconvening to take account of external feedback.

More information about stakeholders' work will be available at: https://www.ntia.doc.gov/other-publication/2018/SoftwareTransparency.

Time and Date: NTIA will convene the first meeting of the multistakeholder process on Software Component Transparency on July 19, 2018, from 10:00 a.m. to 4:00 p.m. Eastern Daylight Time. Please refer to NTIA's website, https://www.ntia.doc.gov/other-publication/2018/SoftwareTransparency, for the most current information.

Place: The meeting will be held at the American Institute of Architects, 1735 New York Ave. N.W., Washington, DC 20006. The location of the meeting is subject to change. Please refer to NTIA's website, https://www.ntia.doc.gov/other-publication/2018/SoftwareTransparency, for the most current information.

Other Information: The meeting is open to the public and the press on a first-come, first-served basis. Space is limited.

The meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Allan Friedman at (202) 482-4281 or afriedman@ntia.doc.gov at least seven (7) business days prior to each meeting. The meetings will also be webcast. Requests for real-time captioning of the webcast or other auxiliary aids should be directed to Allan Friedman at (202) 482-4281 or afriedman@ntia.doc.gov at least seven (7) business days prior to each meeting. There will be an opportunity for stakeholders viewing the webcast to participate remotely in the meetings through a moderated conference bridge, including polling functionality. Access details for the meetings are subject to change. Please refer to NTIA's website, https://www.ntia.doc.gov/other-publication/2018/SoftwareTransparency, for the most current information.

Dated: June 4, 2018.

David J. Redl,

Assistant Secretary for Communication and Information, National Telecommunications and Information Administration.

[FR Doc. 2018-12261 Filed: 6/6/2018 8:45 am; Publication Date: 6/7/2018]